

REMARKS

New claims 18-20 have been added and no claims have been canceled. Accordingly, claims 1-20 are pending in this application. Claim 9 has been amended in order to correct a minor typographical error. No new matter has been added.

Claim Objections

In reference to the claim objection by the Examiner, claims 10-17 were previously renumbered as claims 9-16 in the Preliminary Amendment filed on March 1, 2002. The above Listing of Claims also includes the corrected claim numbers.

35 U.S.C. §§ 102 and 103

Claims 1-17 have been rejected under 35 U.S.C. § 102(b) as being anticipated by Kitamura et al, U.S. Patent No. 6,907,496. Claims 10-11 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kitamura et al in view of Li et al, U.S. Publication No. 2003/0093509. Further, claims 5-7 and 12-17 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kitamura et al in view of Sanada, U. S. Publication No. 2001/0008010. Applicants request reconsideration of the rejections for the following reasons.

As shown in FIG. 1 of the present application, a second storage system or second storage 101 has a disk controller 102 and storage disks, such as hard disk drives 103, 104, and 105 for storing data. An internal network connects the disk controller with the hard disk drives. A network of working group 1 (107) and a network of working group 2 (108) is connected to respective host computers and to network transportation ports 113, 114 of the disk controller. The disk controller 102 receives and interprets I/O commands requested by the host computers 109 to 112, and converts them into a proper form, to issue to the hard disk drives 103 to 105. Access controllers 115 and 116 interpret and execute I/O requests transmitted by the host computers such that when I/O process is transmitted, the access controllers 115 and 116 refer to an access controlling table 123 that stores access

authorization setting information in order to determine whether the I/O commands should be authorized. A management console 124 is used for information display and for an administrator to maintain and control the second storage system 101.

FIG. 2 of the present application shows an example of the access controlling table 123 in which is set access controlling information. The access authorization setting for each logical disk is described in the columns of the example for each network port. A logical disk is realized virtually and may comprise one or more of the hard disk drives and the logical disks are therefore flexible assigned among the hard disk drives. As shown in the table of Fig. 2, I/O commands in which access from the network ports is authorized for each logical disk are described. In particular, the I/O commands authorized from the network port for the logical disk are described in each field of the access controlling table 123. Three types of "READ enable," "WRITE enable" and "-" can be described in the fields. "READ enable" is a READ only enable, and "WRITE enable" is a WRITE only enable, and "-" is to be not recognized by the host computer connected to such network port, i.e. access from the network port is recognition-disabled. See page 11, lines 12-22 of the specification, for example.

FIG. 3 shows a flowchart describing the process involved in the invention when the second storage system 101 receives and executes the I/O commands. In brief, the I/O commands from the host computer reach the network ports and are transmitted to the corresponding access controllers 115 and 116. The access controllers 115 and 116 extract a target logical disk number included in the I/O commands and refer to the access controlling table 123 via the table controller 125. The access controller reads contents of a corresponding field of the access controlling table from the logical disk number and the identifier of the network port and judges whether or not such I/O command is authorized. If it is authorized, then the I/O command is execute and if not, the access controllers 115 and 116 notify the host computer of a failure of the I/O command. Further, in the SCSI standards, when the I/O command is failed, the host computer occasionally issues a "REQUEST SENSE" command which requests error information of the device to the second storage system. The access controllers 115 and 116 also report to the management console 124 that unauthorized access has been gained and this unauthorized access event is logged in a file.

New claims 18-20 include that the access controller processes I/O commands of

different types, e.g. read and write commands that are requested for the transportation ports, and that the access controlling table stores access control setting information for each of the network transportation ports that defines one of unauthorized access for the I/O commands or authorized access for at least one of the types of the I/O commands between each of the plurality of transportation ports and each of the plurality of data storing devices. With reference to the foregoing discussion Applicants respectfully assert that the features of new claims 18-20 are fully supported by the specification and drawings of the present invention.

The Examiner cites Kitamura for disclosing the invention as claimed. Applicants request reconsideration of this determination, however, for the following reasons. In particular, the Office Action states that Kitamura discloses a controller having a plurality of network ports connected to different networks. In Kitamura, a managing host computer 3 has a control manager 31 that is connected to a storage device subsystem. Kitamura is also cited for disclosing an access control for processing I/O commands requested for the network ports. However, in Kitamura, the control manager 31 assigns the storage device systems as set forth in the steps shown in Fig. 4 and then the assigned storage device is used by the host computer. See column 10, lines 3-12 of Kitamura, for example. Accordingly, Kitamura does not disclose an access controller processing I/O commands requested for the network transportation ports, but rather assigns storage devices of the storage subsystems to each of the host computers by setting a port number, target ID and LUN for the storage devices in the volume manager 11 of the respective host computer to which the storage device is assigned. See col. 7, lines 41-47 of the reference.

The claimed combination is different from the Kitamura reference because Applicants set forth an access controller for processing I/O commands using access control information set in an access controlling table of the disk controller to authorize or reject I/O commands requested for the network transportation ports. In claim 1, the access control setting information is claimed as be able to define the I/O commands that are to be authorized between each of the plurality of transportation ports and each of the plurality of nonvolatile data storing means. In Kitamura, the access to the storage devices is set up in accordance with the data registered in the volume manager 11 of the host computer by the managing host computer. Accordingly, Kitamura does not disclose the claimed access controller and access

controlling table for storing access control setting information, as claimed by Applicants in claims 1 and 8.

Claim 8 further sets forth an access controlling method of the second storage according to the present invention. As set forth in claim 8, the access controller for processing I/O commands requested for the network ports refers to the access controlling table and judges whether or not the I/O command is authorized between the network port and one of the nonvolatile data storing means of the second storage. Since Kitamura does not disclose a access controlling table as set forth in claim 8, the claims are not anticipated by the reference. Accordingly, the 35 USC §102(b) of claims 1-3 and 8 should be withdrawn.

The Examiner relies upon Li et al. with respect to disclosing the aspect of the invention set forth in claim 10, which states that when a frequency of judgment that access non-authorization to specific data stored in the nonvolatile data storing means exceeds a predetermined threshold, an administrator of the second storage is notified that the judgment frequency of the access non-authorization exceeds a predetermined threshold. However, Li does not make up for the deficiency in Kitamura with respect to the claimed combination set forth in claim 8 which includes judging whether or not an I/O command is authorized between the network port and the nonvolatile data storing means of the second storage by referring to an access controlling table. Accordingly, the combination of Kitamura and Li does not render the invention as claimed unpatentable under 35 USC §103(a).

Sanada et al. is relied upon in rejecting claims 5-7 and 12-17. In particular Sanada et al. is cited for disclosing an access controlling method which uses an SCSI interface for I/O commands, and which produces a “check condition” status as a report of abnormalities. However, the disclosure of Sanada et al. does not make up for the deficiency in Kitamura with respect to the invention set forth in the independent claims, as aforementioned. Accordingly, the combination of Kitamura and Sanada et al. does not render the invention set forth in claims 5-7 and 12-17 unpatentable under 35 USC §103(a).

New Claims 18-20

New claims 18-20 are patentable over the art of record for the foregoing reasons asserted with respect to the patentability of claims 1-7. Further, claim 18 sets forth that the

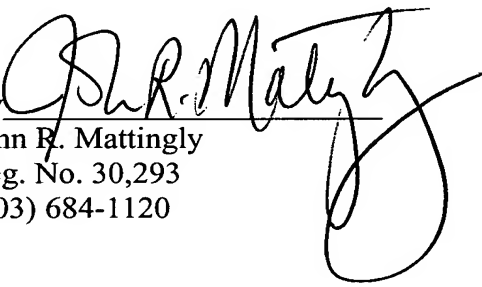
access controller processes I/O commands of different types, e.g. read and write commands that are requested for the transportation ports, and that the access controlling table stores access control setting information for each of the network transportation ports that defines one of unauthorized access for the I/O commands or authorized access for at least one of the types of the I/O commands between each of the plurality of transportation ports and each of the plurality of data storing devices. Thus, the combination of claim 18 is not anticipated or rendered obvious by the art of record and claims 18-20 should be allowed.

CONCLUSION

In view of the foregoing, Applicant respectfully requests that a timely Notice of Allowance be issued in this case.

Respectfully submitted,

MATTINGLY, STANGER, MALUR & BRUNDIDGE, P.C.

By 
John R. Mattingly
Reg. No. 30,293
(703) 684-1120

JRM/so
Date: September 19, 2005